Wazuh & Suricata Implementation Summary

1. Deployment Overview

- Wazuh 4.7 deployed as the central SIEM/XDR platform.

- Suricata 6.0.8 installed as the IDS/IPS for network threat detection.

- 4 Active Agents monitored:

  - 2 Windows endpoints (Win 10/11).

  - 2 Linux hosts (Kali & Ubuntu) running Suricata.

2. Key Tasks Completed

A. Wazuh Setup

- Installed Wazuh Manager (server) and Dashboard (web UI).

- Deployed Wazuh Agents on all endpoints using:

```bash
wget
https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUHL_MANAGER='192.168.1.80' dpkg -i
./wazuh-agent_4.7.5-1_amd64.deb
```

- Verified agent-manager communication.

B. Suricata Integration

- Installed Suricata 6.0.8 on Linux hosts (`kali-suricata`, `ubuntu22_suricata`).

- Configured:

  - Network monitoring rules (`/etc/suricata/suricata.yaml`).

  - Log forwarding to Wazuh via `/var/log/suricata/eve.json`.

- Enabled rule updates:

```bash
sudo suricata-update
```

C. Correlation & Alerting

- Integrated Suricata logs with Wazuh for unified threat detection.

- Tested:

  - Host-based alerts (Wazuh agents).

  - Network-based alerts (Suricata).

3. Current Capabilities

- Real-time monitoring of:

  - Windows system events (malware, logins, etc.).

  - Network threats (intrusions, exploits) via Suricata.

- Centralized dashboard for all security events.

4. Next Steps

- Fine-tune Suricata rules to reduce false positives.

- Configure automated PDF reports in Wazuh.

- Expand agent coverage to additional endpoints.

Key Commands Used

Purpose	Command
Install Wazuh Agent	wget [URL] && sudo WAZUHL_MANAGER='IP' dpkg -i wazuh-agent.deb
Update Suricata Rules	sudo suricata-update
Check Suricata Logs	tail -f /var/log/suricata/eve.json
Verify Wazuh Alerts	tail -f /var/ossec/logs/alerts/alerts.log

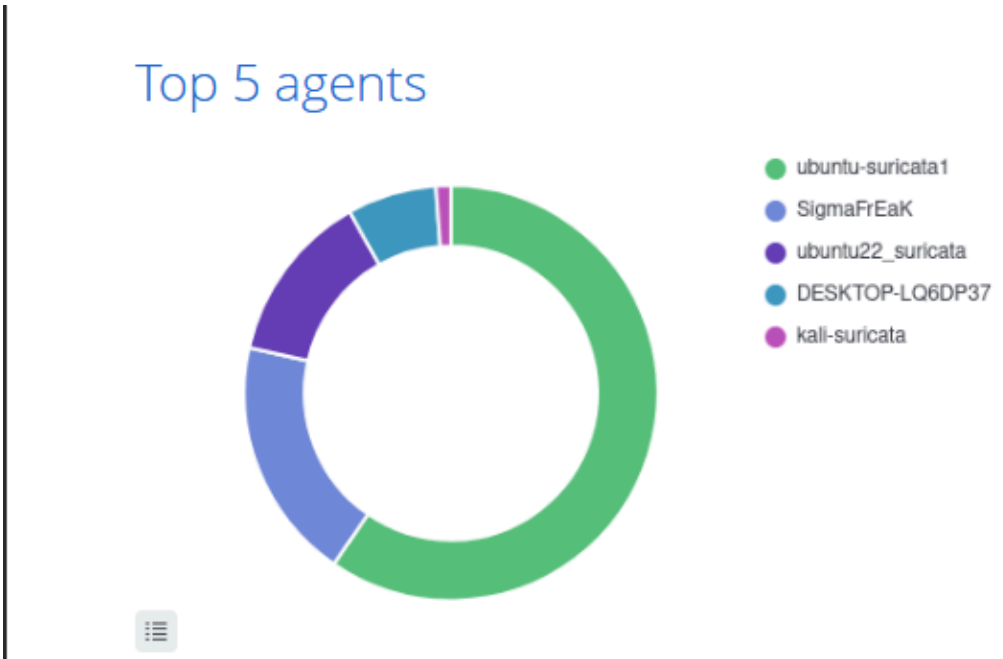
5.Suricata Alerts

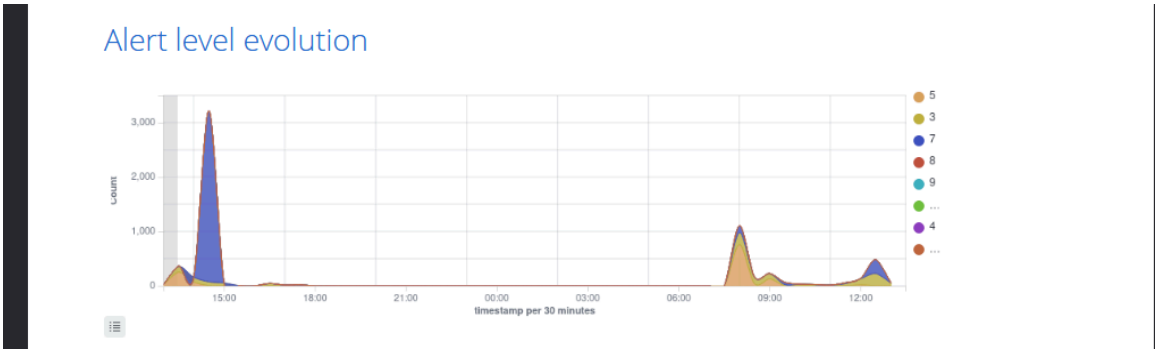
```
Suricata: Alert - GPL ATTACK_RESPONSE id check returned root
```

This alert is popped by our testes to see if everything is working fine :

- curl http://testmynids.org/uid/index.html

6. Screenshots From Wazuh's interface:





Alerts


Modify Registry
Valid Accounts
Data Destruction
File Deletion
Sudo and Sudo Cac...
Stored Data Manipul...
Password Guessing
Network Sniffing
Disable or Modify Tools
S...
Brute Force
Account Manipulation

Rule ID	Description	Level	Count
510	Host-based anomaly detection event (rootcheck).	7	3188
533	Listened ports status (netstat) changed (new port opened or closed).	7	22
5104	Interface entered in promiscuous(sniffing) mode.	8	16
2904	Dpkg (Debian Package) half configured.	7	12
2902	New dpkg (Debian Package) installed.	7	10
60602	Windows application error event.	9	9
2502	syslog: User missed the password more than one time	10	4
60110	User account changed.	8	3
19004	SCA summary: CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Score less than 50% (33)	7	2
19004	SCA summary: CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0: Score less than 50% (39)	7	2
5132	Unsigned kernel module was loaded	11	2
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename administrator account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Accounts: Rename guest account'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message text for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Configure 'Interactive logon: Message title for users attempting to log on'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)').	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Clipboard synchronization across devices' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cloud Search' is set to 'Enabled: Disable Cloud Search'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Cortana' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Diagnostic Data' is set to 'Enabled: Diagnostic data off (not recommended)' or 'Enabled: Send required diagnostic data'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Message Service Cloud Sync' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Online Tips' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Print Spooler to accept client connections' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Remote Shell Access' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow UI Automation redirection' is set to 'Disabled'.	7	1
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Use of Camera' is set to 'Disabled'.	7	1

Rule ID	Description	Level	Count
19007	CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'.	7	1
5712	sshd: brute force trying to get access to the system. Non existent user.	10	1
60776	SessionEnv was unavailable to handle a critical notification event.	7	1

Final Notes

The implementation successfully combines host (Wazuh) and network (Suricata) security monitoring.
Excluded Agent: `ubuntu-suricata1` (192.168.1.95) as it was used for testing issues only .